

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

VICTORIA ANDRETTA, <i>individually and on</i>)	
<i>behalf of all others similarly situated,</i>)	
)	Case No. 1:24-cv-4557
Plaintiff,)	
)	
v.)	
)	
SUMMIT HEALTH MANAGEMENT, LLC)	
D/B/A CITYMD,)	
)	JURY TRIAL DEMANDED
Defendant.)	

CLASS ACTION COMPLAINT

Plaintiff Victoria Andretta (“Plaintiff”),¹ brings this class action lawsuit on behalf of herself, and all others similarly situated, by and through undersigned counsel, and hereby alleges the following against Defendant Summit Health Management, LLC d/b/a CityMD (“Defendant” or “CityMD”). Facts pertaining to Plaintiff and her experiences and circumstances are alleged based upon personal knowledge, and all other facts alleged herein are based upon investigation of counsel and, where indicated, upon information and good faith belief.

NATURE OF THE ACTION

1. Information concerning a person’s physical and mental health is among the most confidential and sensitive information in our society and the mishandling of such information can have serious consequences including, but certainly not limited to, discrimination in the workplace and/or denial of insurance coverage.²

¹ Plaintiff files this Complaint with redactions to protect her health information under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) and New York law.

² See Lindsey Ellefson, Telehealth Sites Put Addiction Patient Data at Risk: New research found pervasive use of tracking tech on substance-abuse-focused health care websites, potentially

2. Simply put, if people do not trust that their protected health information will be kept private and secure, they may be less likely to seek medical treatment which can lead to much more serious health consequences down the road. In addition, protecting medical information and making sure it is kept confidential and not disclosed to any unauthorized entities is vitally necessary to maintain public trust in the healthcare system as a whole.

3. The need for data privacy, security and transparency is particularly acute when it comes to the rapidly expanding world of digital telehealth providers; of all the information the average internet user shares with technology companies, health data is some of the most extensive, valuable and controversial.³

4. Plaintiff brings this class action lawsuit to address CityMD’s illegal and widespread practice of disclosing its patients’ confidential personally identifiable information (“PII”) and protected health information (“PHI”, collectively referred to as “Private Information”) to unauthorized third parties, including Meta Platforms, Inc. d/b/a Meta (“Facebook” or “Meta”) and Google LLC (“Google”).

<https://www.wired.com/story/substance-abuse-telehealth-privacy-tracking-tech/> (last accessed June 1, 2024) (“While the sharing of any kind of patient information is often strictly regulated or outright forbidden, it’s even more verboten in addiction treatment, as patients’ medical history can be inherently criminal and stigmatized.”); *see also* Todd Feathers, Simon Fondrie-Teitler, Angie Waller & Surya Mattu, Facebook Is Receiving Sensitive Medical Information from Hospital Websites, *THE MARKUP* (June 16, 2022), <https://themarkup.org/pixelhunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites> (last visited June 1, 2024).

³ Protected and highly sensitive medical information collected by telehealth companies includes many categories from intimate details of an individual’s conditions, symptoms, diagnoses and treatments to personally identifying information to unique codes which can identify and connect individuals to the collecting entity. *See* Molly Osberg & Dhruv Mehrotra, *The Spooky, Loosely Regulated World of Online Therapy*, JEZEBEL (Feb. 19, 2020), <https://jezebel.com/the-spooky-loosely-regulated-world-of-online-therapy-1841791137> (last visited Jun 13, 2024).

5. Defendant operates over 175 urgent care locations across New York and New Jersey.⁴

6. Defendant also owns and controls citymd.com and its webpages (the “Website”), which Defendant encourages its patients to use to (i) book medical appointments, (ii) locate urgent care facilities, (iii) pay bills, (iv) check insurance coverage, (v) research treatment options and (vi) research specific medical conditions.⁵

7. Defendant’s illegal privacy violations occurred and continue to occur because of the tracking technologies that it installed on its Website including, but not limited to, the Meta Pixel, Google Analytics, Google Tag Manager, Google DoubleClick, Bing (Microsoft) tracking code, BlueCava, LinkedIn cookies and related tools (collectively, “Tracking Technologies”).⁶

8. The Tracking Technologies that Defendant installed and configured allowed unauthorized third parties to intercept the contents of patient communications, view patients’ Private Information, mine that information for purposes unrelated to the provision of healthcare and further monetize it to deliver targeted advertisements to specific individuals.

9. In doing so, and by designing its Website in the manner described throughout this Complaint, CityMD knew or should have known that its patients would use the Website to communicate Private Information while obtaining and receiving medical services.

⁴ See <https://www.citymd.com/health-and-wellness/urgent-care-emergency-room-where-should-i-go#:~:text=Convenience%20E2%80%94%20Our%20locations%20make%20it,you%20can%20just%20walk%20into>. (last visited June 7, 2024).

⁵ <https://www.citymd.com/services/illnesses> (last visited June 6, 2024).

⁶ This Complaint contains images and evidence demonstrating the Meta Pixel was used on Defendant’s Website, but Plaintiff (without the benefit of discovery) does not have access to every tracking tool that was previously installed on the Website.

10. Operating as designed and as implemented by Defendant, the Tracking Technologies, including the Meta Pixel, allowed the Private Information that Plaintiff and Class Members submitted to Defendant to be unlawfully disclosed to Facebook alongside their unique and persistent Facebook ID, IP address and other static identifiers in violation of HIPAA, state laws, industry standards and patient expectations.

11. By installing Tracking Technologies on its Website, Defendant effectively planted a bug in Plaintiff's and Class Members' web browsers that caused their communications to be intercepted, accessed, viewed and captured by third parties in real time, as they were communicated by patients based on the parameters Defendant chose to implement.

12. In 2022 the Office for Civil Rights ("OCR" at the U.S. Department of Health and Human Services ("HHS")) issued a Bulletin to highlight the obligations of HIPAA covered entities and business associates when using online tracking technologies (the "Bulletin").⁷ The Bulletin expressly provides that "[r]egulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules" (emphasis in original).⁸

13. On March 18, 2024, OCR updated its guidance "to increase clarity for regulated entities and the public",⁹ reinforcing the underlying thesis of this Complaint—that Defendant's implementation of Tracking Technologies violates HIPAA.

⁷ See *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html> (last visited June 6, 2024).

⁸ *Id.*

⁹ *Id.*

14. Plaintiff and Class Members used Defendant’s Website to submit information related to their past, present or future health conditions, including, for example, searches for treatment and the booking of medical appointments. Such Private Information allows a third party, such as Facebook or Google, to know that a specific patient was seeking confidential medical care from Defendant as well as the type of medical care being sought.

15. Simply put, the health information disclosed through the Tracking Technologies is personally identifiable.

16. Defendant is a healthcare entity and thus its disclosure of health and medical communications is tightly regulated. HHS has established “Standards for Privacy of Individually Identifiable Health Information” (also known as the “Privacy Rule”) governing how health care providers must safeguard and protect Private Information. Under the HIPAA Privacy Rule, no health care provider may disclose a person’s personally identifiable protected health information to a third party without express written authorization.

17. Healthcare patients simply do not anticipate or expect that their trusted healthcare provider will send PHI or confidential medical information collected via its webpages to a hidden third party—let alone Facebook and Google, which both have a sordid history of privacy violations in pursuit of ever-increasing advertising revenue—without the patients’ consent. Neither Plaintiff nor any other Class Member signed a written authorization permitting Defendant to send their Private Information to Facebook or Google.

18. And as noted by the Honorable William J. Orrick in a decision concerning the use of the Facebook Pixel by healthcare organizations,

Our nation recognizes the importance of privacy in general and health information in particular: the safekeeping of this sensitive information is enshrined under state and federal law. The allegations against Meta are troubling: Plaintiff raise potentially strong claims

on the merits and their alleged injury would be irreparable if proven.¹⁰

19. Consequently, Plaintiff brings this action for legal and equitable remedies to address and rectify the illegal conduct and actions described herein, to enjoin Defendant from making similar disclosure of its patients' Private Information in the future, and to fully articulate, *inter alia*, the specific Private Information it disclosed to third parties and to identify the recipients of that information.

20. Defendant breached its statutory and common law obligations to Plaintiff and Class Members by, *inter alia*,: (i) installing and configuring, and then failing to remove or disengage, technology that was known and designed to share web-users' information; (ii) failing to obtain the written consent of Plaintiff and Class Members to disclose their Private Information to Facebook or others; (iii) failing to take steps to block the transmission of Plaintiff's and Class Members' Private Information through Tracking Technologies like the Meta Pixel or Google Analytics; (iv) failing to warn Plaintiff and Class Members; and (v) otherwise failing to design and monitor its Website to maintain the confidentiality and integrity of patient Private Information.

21. As a result of Defendant's conduct, Plaintiff and Class Members have suffered numerous injuries including, but not limited to: (i) invasion of privacy; (ii) loss of benefit of the bargain, (iii) diminution of value of their Private Information, (iv) statutory damages and (v) the continued and ongoing risk to their Private Information.

22. Plaintiff seeks to remedy these harms and brings causes of action for (i) violation of the Electronics Communication Privacy Act ("ECPA"), 18 U.S.C. § 2511(1), *et seq.*; (ii) breach of implied contract; (iii) negligence; (iv) breach of confidence; (v) constructive bailment; (vi)

¹⁰ *In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d 778, 783 (N.D. Cal. 2022).

violation of the New York Deceptive Trade Practices Act New York Gen. Bus. Law § 349, *et seq.*; (vii) and unjust enrichment.

PARTIES

23. Plaintiff Victoria Andretta is, and at all relevant times was, an individual residing in New York City, New York County, in the State of New York.

24. In 2019, CityMD and Summit Medical Group finalized a merger agreement that created a single entity, known as Summit Health.¹¹

25. Defendant operates numerous urgent care centers throughout the states of New York and New Jersey under the names Summit Medical Group and CityMD, which operate together as Summit Health.

26. Defendant Summit Health Management, LLC is a domestic corporation incorporated in the State of New Jersey.

27. CityMD is a provider of urgent care services and maintains a corporate headquarters at 1345 Avenue of the Americas, New York City, New York, 10105-0302.

28. Defendant is a covered entity under HIPAA.

JURISDICTION & VENUE

29. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1331 because this Complaint asserts a claim for violation of federal law, specifically, the ECPA, 18 U.S.C. § 2511. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

¹¹ See CityMD and Summit Health Finalize Merger, (Aug. 13, 2019), <https://www.summithealth.com/news/citymd-and-summit-health-finalize-merger> (last visited June 7, 2024)

30. This Court also has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this case is brought as a class action where the amount in controversy exceeds the sum or value of \$5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

31. This Court has personal jurisdiction over CityMD because the parties are citizens of different states and the amount in controversy exceeds \$75,000, 28 U.S.C. § 1332(a)(1), Defendant is authorized to and regularly conducts business in this judicial district, and CityMD's principal place of business is in the state of New York.

32. Venue is proper under 28 U.S.C § 1391(b)(2) because a substantial part of the events or omissions which gave rise to these claims occurred in this district and because CityMD's principal place of business is in this district.

COMMON FACTUAL ALLEGATIONS

A. Background

33. Facebook operates the world's largest social media company and generated \$117 billion in revenue in 2021, roughly 97% of which was derived from selling advertising space.¹²

34. In conjunction with its advertising business, Facebook encourages and promotes entities and website owners, such as Defendant, to utilize its "Business Tools" to gather, identify, target, and market products and services to individuals.

¹²*Facebook, Meta Reports Fourth Quarter and Full Year 2021 Results*, FACEBOOK, <https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx> (last visited June 6, 2024).

35. Facebook’s Business Tools, including the Pixel and Conversions API, are bits of code that advertisers can integrate into their webpages, mobile applications and servers, thereby enabling the interception and collection of website visitors’ activity.

36. Specifically, the Pixel “tracks the people and type of actions they take.”¹³ When a user accesses a webpage hosting the Pixel, their communications with the host webpage are instantaneously and surreptitiously duplicated and sent to Facebook’s servers. Notably, this transmission does not occur unless the webpage contains the Pixel.

37. The Pixel is customizable and programmable, meaning that the website owner controls which of its web pages contain the Pixel and which events are tracked and transmitted to Facebook.

38. The process of adding the Pixel to webpages is a multi-step process that must be undertaken by the website owner.¹⁴

39. Facebook guides the website owner through setting up the Pixel during the setup process. Specifically, Facebook explains that there are two steps to set up a pixel: “(1) Create your pixel and set up the pixel base code on your website. You can use a partner integration if one is available to you or you can manually add code to your website. (2) Set up events on your website to measure the actions you care about, like making a purchase. You can use a partner integration, the point-and-click event setup tool, or you can manually add code to your website.”¹⁵

¹³ RETARGETING, <https://www.facebook.com/business/goals/retargeting> (last visited June 6, 2024).

¹⁴ Business Help Center: How to set up and install a Meta Pixel, <https://www.facebook.com/business/help/952192354843755?id=1205376682832142> (last visited June 6, 2024).

¹⁵ *Id.*

40. Aside from the various steps to embed and activate the Pixel, website owners, like Defendant, must also agree to Facebook’s Business Tools Terms by which Facebook requires website owners using the Pixel to “represent and warrant” that they have adequately and prominently notified users about the collection, sharing and usage of data through Facebook’s Business Tools (including the Pixel) and that websites “will not share Business Tool Data . . . that [websites] know or reasonably should know . . . includes health, financial information or other categories of sensitive information”¹⁶

41. Stated differently, Plaintiff’s and Class Members’ Private Information would not have been disclosed to Facebook but for the Defendant’s decision to install the tracking technologies on its Website.

42. As explained in more detail below, this secret transmission to Facebook is initiated by Defendant’s source code concurrently with Plaintiff’s and Class Members’ communications to their intended recipient, Defendant.

B. CityMD Assisted Third Parties in Intercepting Patients’ Communications with its Website and Disclosed Their Private Information to Third Parties.

43. Defendant’s Website is accessible on mobile devices and desktop computers and allows patients to communicate with Defendant regarding their PHI, medical care and bill payment.

44. Defendant encouraged patients to use its Website to communicate their Private Information, schedule appointments, access information about their treatments, pay medical bills and more.

¹⁶ *Id.*; see also Pratyush Deep Kotoky, *Facebook collects personal data on abortion seekers: Report* (June 16, 2022) <https://www.newsbytesapp.com/news/science/facebook-collects-personaldata-on-abortion-seekers/story> (quoting Facebook spokesman Dale Hogan as saying that it is “against [Facebook’s] policies for websites and apps to send sensitive health data about people through [its] Business Tools”) (last visited June 1, 2024).

45. Despite this, Defendant purposely installed Tracking Technologies, including the Meta Pixel, on its Website and programmed specific webpage(s) to surreptitiously share its patients' private and protected communications, including Plaintiff's and Class Members' PHI and/or PII, which was sent to Facebook, Google and other third parties.

46. The Tracking Technologies followed, recorded and disseminated patients' information as they navigated and communicated with Defendant via the Website, simultaneously transmitting the substance of those communications to unintended and undisclosed third parties.

47. The information disseminated by the Tracking Technologies and/or intercepted by third parties constitutes Private Information including medical information patients requested or viewed, the title of any buttons clicked (such as the "Women's Health" dropdown button under "Services," which indicates the patient has signaled a desire for treatment specifically for women's health issues), the exact phrases typed into text boxes, other selections made from drop-down menus or while using other sensitive and confidential information, the divulgence of which is and was highly offensive to Plaintiff.

48. As described by the OCR Bulletin, this is PHI because the webpages have access to "information that relates to any individual's past, present, or future health, health care, or payment for health care."¹⁷

49. The information collected and disclosed by Defendant's Tracking Technologies is not anonymous and is viewed and categorized by the intercepting party upon receipt.

50. The information Facebook received via the Meta Pixel was linked and connected to patients' Facebook profiles (via their Facebook ID or "c_user id"), which includes other PII.

¹⁷ See OCR Bulletin *supra*, note 7.

51. Similarly, through the Tracking Technologies, Google stores users' logged-in identifier on non-Google websites in its logs. Whenever a user logs-in on non-Google websites, whether in private browsing mode or non-private browsing mode, the same identifier is associated with the data Google collects from the user's browsing activities on that website. Google further logs all such data (private and non-private) within the same logs and uses these data for serving personalized ads.

52. Simply put, the health information that was disclosed via the Tracking Technologies is personally identifiable and was sent alongside other persistent unique identifiers such as the patients' IP address, Facebook ID and device identifiers.¹⁸

C. CityMD's Tracking Technologies, Source Code, Interception of HTTP Requests and Transmission of HTTP Requests.

53. Web browsers are software applications that allow consumers to navigate the internet and exchange electronic communications, and every "client device" (computer, tablet or smart phone) has a web browser (e.g., Microsoft Edge, Google Chrome, Mozilla's Firefox, etc.).

54. Every website is hosted by a computer "server" which allows the website's owner (Defendant) to display the Website and exchange communications with the website's visitors (Plaintiff and Class Members) via the visitors' web browser.

55. When patients used Defendant's Website, they engaged in an ongoing back-and-forth exchange of electronic communications with Defendant wherein their web browser communicated with Defendant's computer server—like how two telephones communicate.

¹⁸ See *Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1056 (N.D. Cal. 2021) (discussing how Google collects personal information and IP addresses); see also <https://developers.facebook.com/docs/meta-pixel/> (last visited June 7, 2024).

56. These communications are invisible to ordinary consumers,¹⁹ but one browsing session may consist of thousands of individual HTTP Requests and HTTP Responses.

57. A patient's HTTP Request essentially asks the Defendant's Website to retrieve certain information (such as a "Find a CityMD" webpage), and the HTTP Response renders or loads the requested information in the form of "Markup" (the pages, images, words, buttons and other features that appear on the patient's screen as they navigate Defendant's Website).

58. Every webpage is comprised of both Markup and "source code." Source code is simply a set of instructions that commands the website visitor's browser to take certain actions when the web page first loads or when a specified event triggers the code.

59. Defendant's Tracking Technologies were embedded in its Website's source code, which is contained in its HTTP Response. The Tracking Technologies, which were programmed to automatically track patients' communications and transmit them to third parties, executed instructions that effectively opened a hidden spying window into each patients' web browser, through which third parties intercepted patients' communications and activity.

60. For example, when a patient visits www.citymd.com and selects the "Virtual Care" or "Get Care Now" button, the patient's browser automatically sends an HTTP Request to Defendant's web server. Defendant's web server automatically returns an HTTP Response, which loads the Markup for that particular webpage. As depicted below, the user only sees the Markup, not Defendant's source code or underlying HTTP Requests and Responses.

¹⁹ See OCR Bulletin *supra*, note 7 ("Tracking technologies collect information and track users in various ways, many of which are not apparent to the website or mobile app user.").

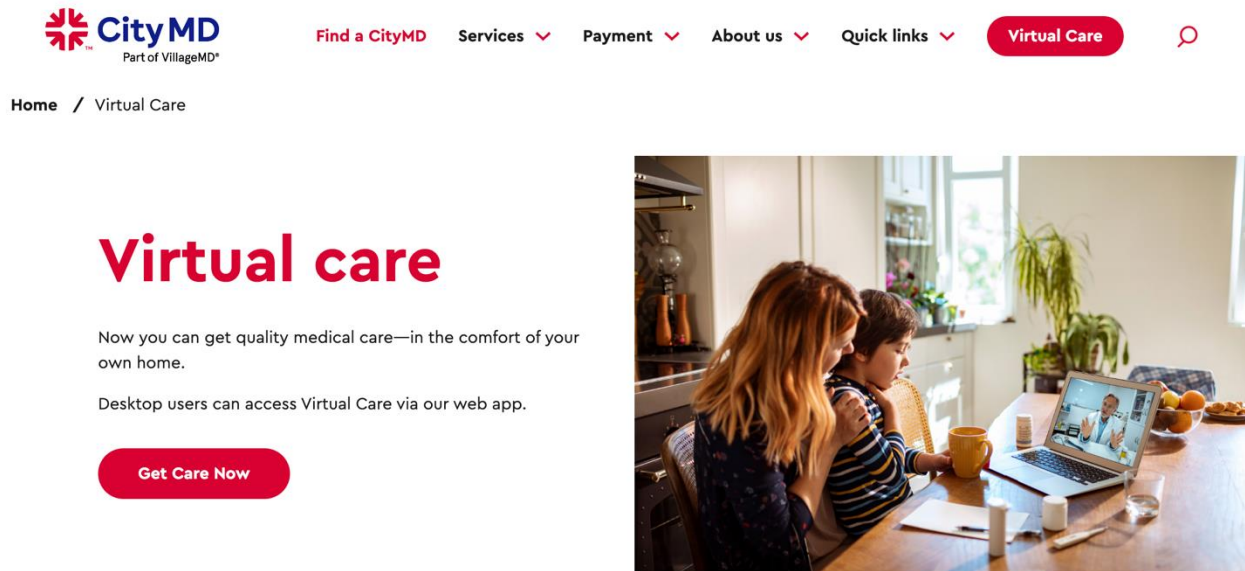


Figure 1. The image above is a screenshot taken from the user's web browser upon visiting <https://www.citymd.com/virtualcare>

61. The image above displays the Markup of Defendant's webpage. Behind the scenes, however, Tracking Technologies like the Meta Pixel and Google Analytics are embedded in the source code, automatically transmitting everything the patient does on the webpage and effectively opening a hidden spy window into the patients' browser.

D. Defendant Disclosed Plaintiff's and Class Members' Private Information to Facebook and Google Using Tracking Technologies.

62. In this case, Defendant employed Tracking Technologies to intercept and disclose Plaintiff's and Class Members' Private Information to Facebook, Google and other third parties.

63. Defendant's source code manipulates the patient's browser by secretly instructing it to send the patient's communications (HTTP Requests) with Defendant to Facebook and Google. These transmissions occur contemporaneously, invisibly and without the patient's knowledge.

64. Thus, without its patients' consent, Defendant uses its source code to commandeer and "bug" or "tap" its patients' computing devices, allowing Facebook, Google and other third

parties to listen in on all of their communications with Defendant and thereby intercept those communications, including Private Information.

65. The Tracking Technologies allow Defendant to optimize the delivery of ads, measure cross-device conversions, create custom audiences and decrease advertising and marketing costs. However, Defendant's Website does not rely on the Tracking Technologies to function.

66. While seeking and using Defendant's services as a medical provider, Plaintiff and Class Members communicated their Private Information to Defendant via its Website.

67. Plaintiff and Class Members were not aware that their Private Information would be disclosed to third parties as it was communicated to Defendant because, amongst other reasons, Defendant did not disclose this fact.

68. Plaintiff and Class Members never consented, agreed, authorized or otherwise permitted Defendant to disclose their Private Information to third parties, nor did they intend for anyone other than Defendant to be a party to their communications (many of them highly sensitive and confidential) with Defendant.

69. Defendant's Tracking Technologies sent non-public Private Information to third parties like Facebook and Google, including but not limited to Plaintiff's and Class Members': (i) status as medical patients; (ii) health conditions; (iii) medical treatments; (iv) locations where treatment was sought; (v) bill payment and/or insurance coverage information and (vi) and search queries, such as searches for medical treatment options and medical information specific to patients' medical conditions.

70. Importantly, the Private Information that Defendant's Tracking Technologies sent to third parties included PII that allowed those third parties to connect the Private Information to

a specific patient. Information sent to Facebook was sent alongside the Plaintiff's and Class Members' Facebook ID, thereby allowing individual patients' communications with Defendant and the Private Information contained in those communications to be linked to their unique Facebook accounts and therefore their identity.²⁰

71. A user's Facebook ID is linked to their Facebook profile, which contains a wide range of demographic and other information about the user including, but not limited to, location, pictures, personal interests, work history and relationship status. Because the user's Facebook ID uniquely identifies an individual's Facebook account, Facebook—or any ordinary person—can easily use the Facebook ID to locate, access and view the user's corresponding Facebook profile.

72. Defendant deprived Plaintiff and Class Members of their privacy rights when it: (i) implemented Tracking Technologies that surreptitiously tracked, recorded and disclosed Plaintiff's and other patients' confidential communications and Private Information; (ii) disclosed patients' protected information to unauthorized third parties and (iii) undertook this pattern of conduct without notifying Plaintiff or Class Members and without obtaining their express written consent.

73. By installing and implementing both Facebook tools and Google Analytics, Defendant caused Plaintiff's and Class Member's communications to be intercepted by and/or disclosed to Facebook and Google and for those communications to be personally identifiable.

74. As explained below, these unlawful transmissions are initiated by Defendant's source code concurrent with communications made via certain webpages.

²⁰ Defendant's Website tracks and transmits data via first-party and third-party cookies. The c_user cookie or Facebook ID is a type of third-party cookie assigned to each person who has a Facebook account, and it is comprised by a unique and persistent set of numbers.

E. Defendant's Tracking Technologies Disseminate Patient Information Via Its Website.

75. If a patient uses Defendant's Website to find care, the Website directs them to communicate Private Information, including but not limited to the reason (i.e. the medical condition and/or symptoms) for seeking care, exact search terms entered into the search bar, type of visit (office or virtual), location of that visit, and their status as medical patients.

76. Unbeknownst to the patient, these communications are sent to Facebook and other third-party entities via Defendant's Tracking Technologies.

77. In the example below, the user navigated to the "Find a CityMD" page on Defendant's Website where the user is prompted by Defendant's Website to find a location by inputting personal information regarding their location:

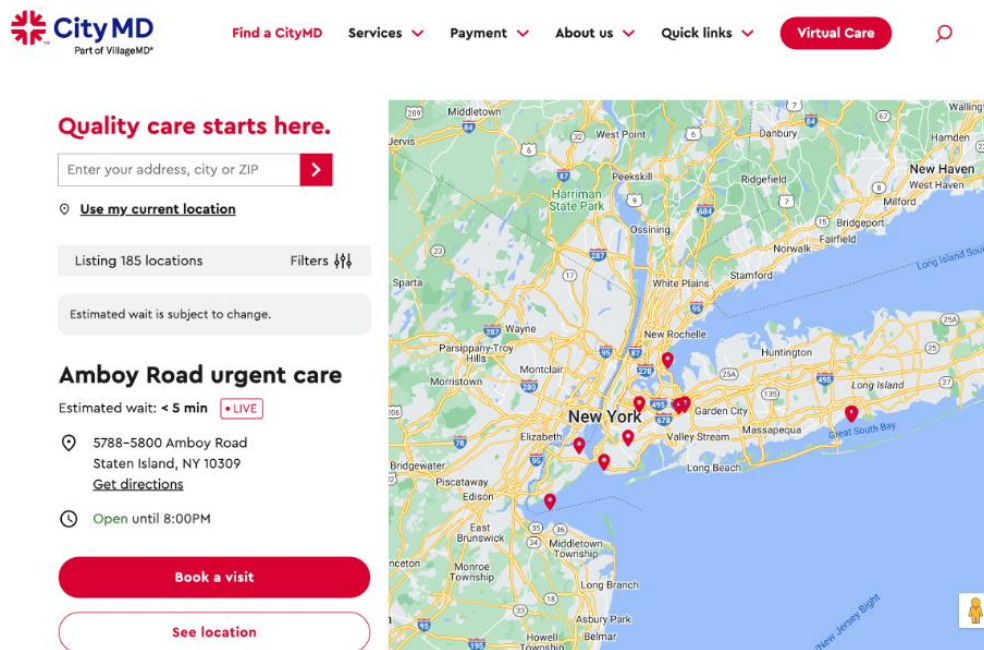


Figure 2. Screenshot taken from citymd.com/urgent-care-locations as the user searches for a location and communicates information via the search bar.

78. In this instance, the user searched for a location near their home address.

79. Unbeknownst to patients, this webpage—which is used to communicate Private Information for the purpose of seeking medical treatment—contains Defendant's Tracking

Technologies. The image below shows the “behind the scenes” portion of the website that is invisible to ordinary users:

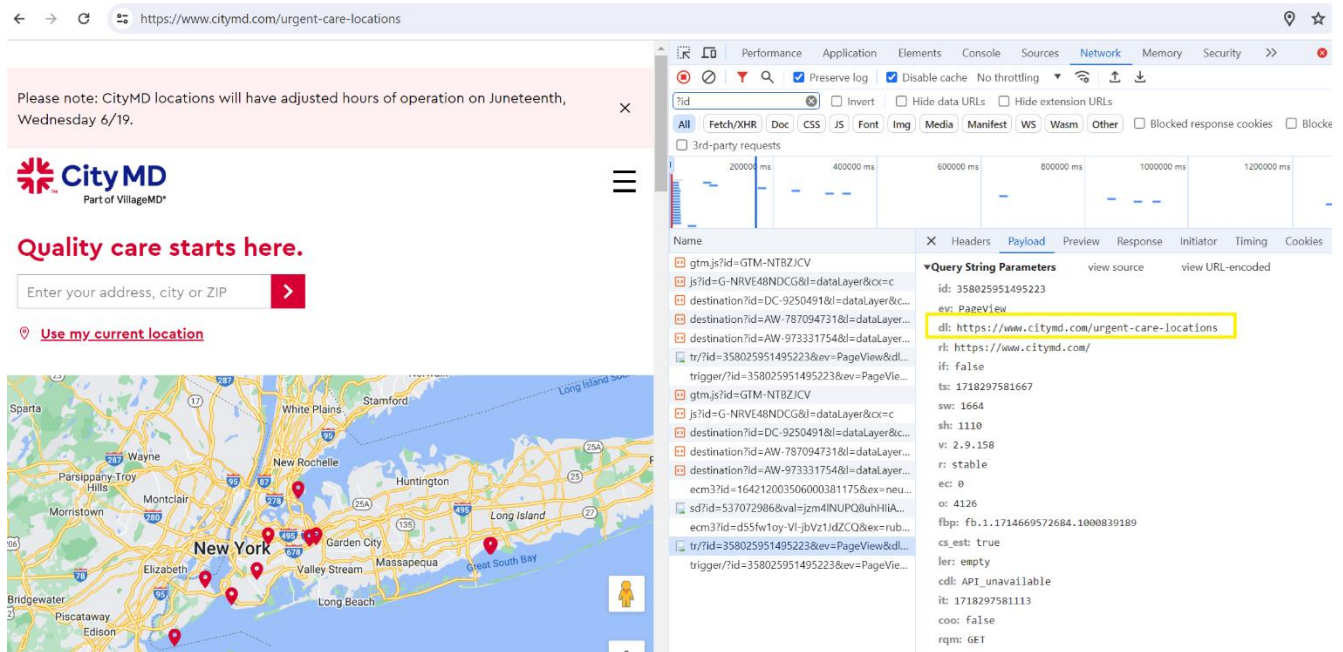


Figure 3. Screenshot from Defendant’s Website depicting back-end network traffic which reveals that the user is searching for CityMD locations.

80. Thus, without alerting the user, Defendant’s Tracking Technologies send the user’s communications via the webpage to Facebook and other third-parties, and the images below confirm that the communications Defendant sends to Facebook contain the user’s Private Information.

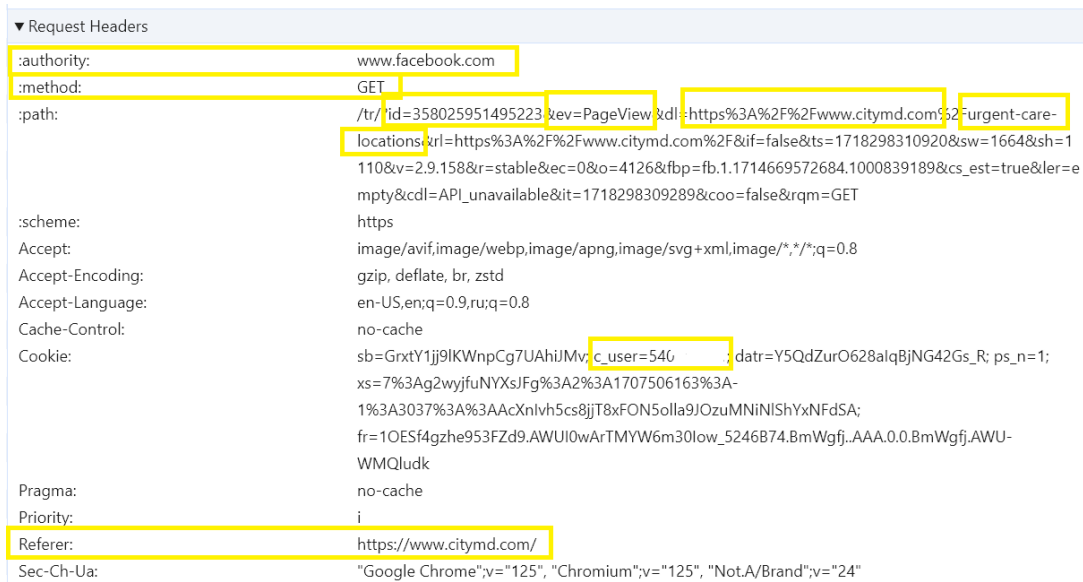


Figure 4: Screenshot from the Network traffic report depicting the data sent to Facebook including specific user identifiers.

81. The first line of highlighted text, “id=358025951495223” refers to Defendant’s Meta Pixel ID and confirms that it implemented the Pixel into its source code for this webpage and transmitted info to Facebook from this webpage.

82. On the same line of text, “ev= PageView,” identifies and categorizes which actions the user took on the webpage (“ev=” is an abbreviation for event, and “PageView” is the type of event). Thus, this identifies the user as having navigated to the Website page.

83. Under request headers, the referrer is highlighted showing that Defendant sent the information to Facebook.

84. Finally, the highlighted text (“GET”) demonstrates that Defendant’s Pixel sent the user’s communications, and the Private Information contained therein, alongside the user’s Facebook ID (c_user ID), thereby allowing the user’s communications and actions on the website to be linked to their specific Facebook profile.

85. The image demonstrates that the user's Facebook ID (highlighted as "c_user=" in the image above) was sent alongside the other data.²¹

86. Once the User selected a specific location, Defendant discloses that to Facebook as well:

```
www.facebook.com
GET
/tr/?id=358025951495223&ev=PageView&dl=https%3A%2F%2Fcitymd.com%2Furgent-care-locations%2Fny%2Fbed-
stuy&rl=https%3A%2F%2Fcitymd.com%2Furgent-care-
locations&if=false&ts=1718301295339&sw=1920&sh=1080&v=2.9.158&r=stable&ec=0&o=4126&fbp=fb.1.171829992364
7.3914609973775085&cs_est=true&ler=empty&cld=API_unavailable&it=1718301295256&coo=false&rqm=GET
https
image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
gzip, deflate, br, zstd
en-US,en;q=0.9
sb=SS1rZp-Drg5IVCRKFTA3bQA; datr=SS1rZn0lubTQwzkReFEZOLuf; locale=en_US; c_user=61560564045991;
xs=3%3AfD1GP9t6TbTGrA%3A2%3A1718300216%3A-1%3A-1; ps_n=1;
fr=0vbOhFaz3aPbghfXm.AWVv52GBpAC5neUol2tqgtMX4uk.Bmay1J..AAA.0.0.BmazCe.AWXJKQvOvLc
```

Figure 5. Disclosure of the User's search & selection of CityMD's location in Bed-Stuyvesant.

87. Defendant's Website offers patients the option of selecting various types of specific services, including from such categories as "injuries," "illnesses," "on-the-job injuries," "women's health," and "occupational medicine."²²

88. In some categories of services offered by Defendant, a User can select even more specific conditions, such as:

- a. "UTI testing,"
- b. "asthma treatment," or

²¹ The user's Facebook ID is represented as the c_user ID highlight in the image below, and it is redacted in the corresponding string of numbers to preserve the user's anonymity.

²² See <https://www.citymd.com/services> (last visited Jun. 13, 2024).

c. “COVID-19.”²³

89. Defendant discloses these searches by its patients to Facebook, as illustrated below:

```

www.facebook.com
GET
/tr/?id=358025951495223&ev=PageView&dl=https%3A%2F%2Fcitymd.com%2Foccupational-medicine%2Fwork-related-
injury-care&url=https%3A%2F%2Fcitymd.com%2Foccupational-
medicine&if=false&ts=1718301854668&sw=1920&sh=1080&v=2.9.158&r=stable&ec=0&o=4126&fbp=fb.1.171829992364
7.3914609973775085&cs_est=true&ler=empty&cdl=API_unavailable&it=1718301854637&coo=false&rqm=GET
https
image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
gzip, deflate, br, zstd
en-US,en;q=0.9
sb=SS1rZp-Drg5IVCRKFTAH3bQA; datr=SS1rZn0lubTQwzkREfEZOLuf; locale=en_US; c_user=61560564045991;

www.facebook.com
GET
/tr/?id=358025951495223&ev=PageView&dl=https%3A%2F%2Fcitymd.com%2Fservices%2Fillnesses%2Fasthma-
treatment&url=https%3A%2F%2Fcitymd.com%2Fservices%2Fillnesses&if=false&ts=1718301953610&sw=1920&sh=1080&v=
2.9.158&r=stable&ec=0&o=4126&fbp=fb.1.1718299923647.3914609973775085&cs_est=true&ler=empty&cdl=API_unavaila
ble&it=1718301953460&coo=false&rqm=GET
https
image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
gzip, deflate, br, zstd
en-US,en;q=0.9
sb=SS1rZp-Drg5IVCRKFTAH3bQA; datr=SS1rZn0lubTQwzkREfEZOLuf; locale=en_US; c_user=61560564045991;

```

²³ See <https://www.citymd.com/services/womens-health/uti-testing>; <https://www.citymd.com/services/illnesses> (last visited Jun. 13, 2024).

```

www.facebook.com
GET
/tr/?id=358025951495223&ev=PageView&dl=https%3A%2F%2Fcitymd.com%2Fservices%2Fwomens-health%2Futi-
testing&rl=https%3A%2F%2Fcitymd.com%2Fservices%2Fwomens-
health&if=false&ts=1718301149913&sw=1920&sh=1080&v=2.9.158&r=stable&ec=0&o=4126&fbp=fb.1.1718299923647.3
914609973775085&cs_est=true&ler=empty&cld=API_unavailable&it=1718301149857&coo=false&rqm=GET
https
image/avif,image/webp,image/apng,image/svg+xml,image/*/*/*;q=0.8
gzip, deflate, br, zstd
en-US,en;q=0.9
sb=SS1rZp-Drg5IVCRKFTAH3bQA; datr=SS1rZn0lubTQwzkREfEZOLuf; locale=en_US; c_user=61560564045991;
xs=3%3AfD1GP9t6TbTGrA%3A2%3A1718300216%3A-1%3A-1; ps_n=1;
fr=0vbOhFaz3aPbghfXm.AWVv52GBpAC5neUol2tqgtMX4uk.Bmay1J..AAA.0.0.BmazCe.AWXJKQvOvLc
i
https://citymd.com/

```

Figures 6-8. Examples of Users' searches for CityMD's services related to their specific medical conditions, along with the User's unique personal identifier, the c_user cookie.

90. Defendant also discloses when a User makes a payment for CityMD's services:

```

www.facebook.com
GET
/tr/?
id=358025951495223&ev=PageView&dl=https%3A%2F%2Fcitymd.com%2Fpayment&rl=https%3A%2F%
2Fcitymd.com%2Fabout&if=false&ts=1718301542215&sw=1920&sh=1080&v=2.9.158&r=stable&ec=0&
o=4126&fbp=fb.1.1718299923647.3914609973775085&cs_est=true&ler=empty&cld=API_unavailable&it
=1718301542084&coo=false&rqm=GET
https
image/avif,image/webp,image/apng,image/svg+xml,image/*/*/*;q=0.8
gzip, deflate, br, zstd
en-US,en;q=0.9
sb=SS1rZp-Drg5IVCRKFTAH3bQA; datr=SS1rZn0lubTQwzkREfEZOLuf; locale=en_US;
c_user=61560564045991; xs=3%3AfD1GP9t6TbTGrA%3A2%3A1718300216%3A-1%3A-1; ps_n=1;

```

Figure 9. Defendant's disclosure of a User's Private Information, including patient status and personal identifiers, when they review their payment options on the Website.

91. To make matters worse, Defendant's Tracking Technologies even track and record the exact text and phrases that a user types into the general search bar located on Defendant's homepage. In the example below, the user typed "I have cancer" into the search bar.

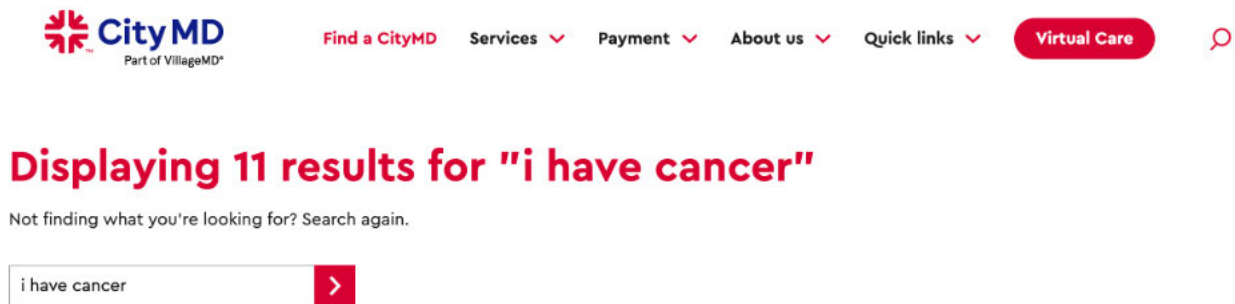


Figure 10. Screenshot from Defendant's Website's search bar feature.

92. That exact phrase is sent to Facebook, thereby allowing the user's medical condition to be linked to their individual Facebook account for future retargeting and exploitation. There is no legitimate reason for sending this information to Facebook.

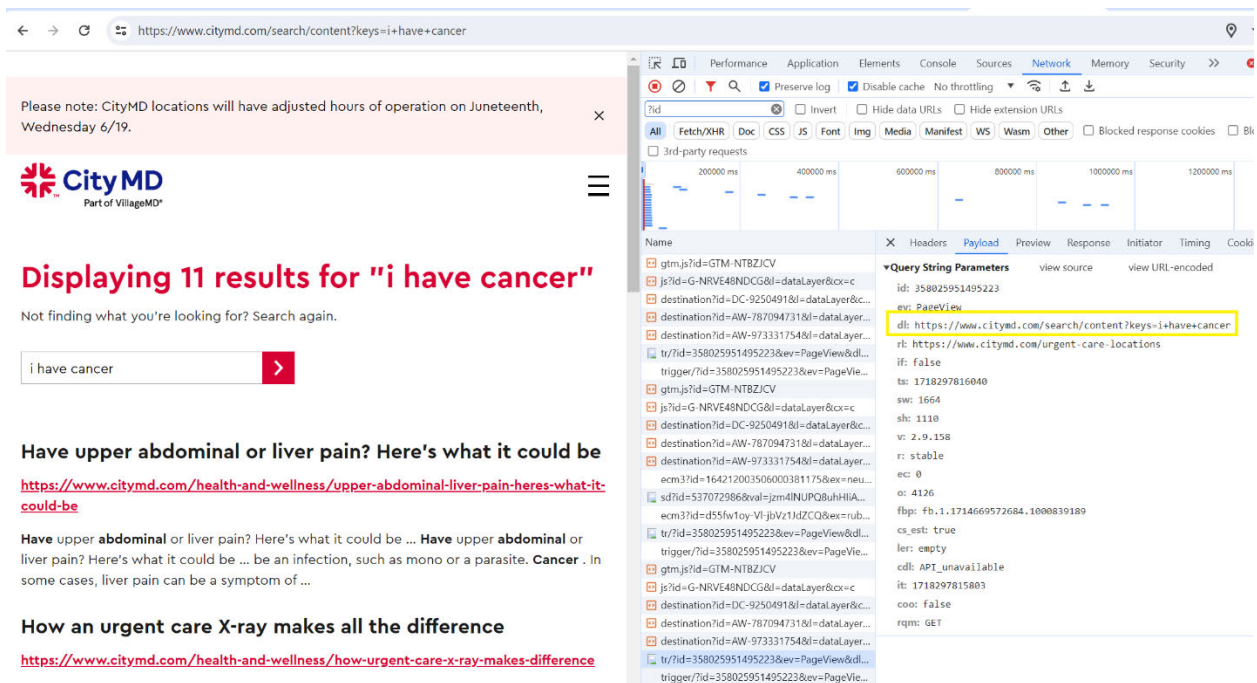


Figure 11. Example of the disclosure of the user's exact search terms "I have cancer" from the Defendant's search bar to Facebook.



Figure 12. Screenshot from Defendant's Website's traffic report of request headers that are sent to Facebook from the Defendant after a user uses the Defendant's search feature.

93. In each of the examples above, the user's website activity and the contents of their communications are sent to Facebook alongside their PII. Marketers and other third parties are able to personally identify individual website users through several means, but the examples above demonstrate what happens when the website user is logged into Facebook on their web browser or device. When this happens, the website user's identity is revealed via third-party cookies that work in conjunction with the Tracking Technologies.

94. For example, the Meta Pixel transmits the user's `c_user` cookie, which contains that user's unencrypted Facebook ID, and allows Facebook to link the user's online communications and interactions to their individual Facebook profile.

95. Facebook receives at least seven cookies when Defendant's website transmits information via the Pixels:

Name ▲	Value	Domain
c_user	540643061	.facebook.com
datr	Y5QdZurO628alqBjNG42Gs_R	.facebook.com
fr	1OESf4gzhe953FZd9.AWUI0wArTMYW6m...	.facebook.com
ps_l	1	.facebook.com
ps_n	1	.facebook.com
sb	GrxtY1jj9lKWnpCg7UAhiJMv	.facebook.com
xs	7%3Ag2wyjfuNYXsJFg%3A2%3A1707506...	.facebook.com

Figure 13. Screenshot of network analysis showing cookies sent to Facebook when a user visits CityMD.com.

96. When a visitor's browser has recently logged out of an account, Facebook compels the visitor's browser to send a smaller set of cookies:²⁴

fr	00Zp...	.facebook.com
wd	1156...	.facebook.com
sb	qqAz...	.facebook.com
datr	Malz...	.facebook.com

Figure 14. Screenshot of cookies for a recently signed out Facebook user.

97. The fr cookie contains an encrypted Facebook ID and browser identifier.²⁵ Facebook, at a minimum, uses the fr cookie to identify users, and this cookie can stay on a user's website browser for up to 90 days after the user has logged out of Facebook.²⁶

²⁴ The screenshot below serves as example and demonstrates the types of data transmitted during an HTTP single communication session. Not pictured here and in the preceding image is the _fbp cookie, which is transmitted as a first-party cookie.

²⁵ Data Protection Commissioner, *Facebook Ireland Ltd: Report of Re-Audit* (Sept. 21, 2012), p. 33, http://www.europe-v-facebook.org/ODPC_Review.pdf (last visited May 23, 2024).

²⁶ *Cookies & other storage technologies*, <https://www.facebook.com/policy/cookies/> (last visited May 23, 2024).

98. At each stage, Defendant also utilizes the `_fbp` cookie, which attaches to a browser as a first-party cookie, and which Facebook uses to identify a browser and a user.²⁷

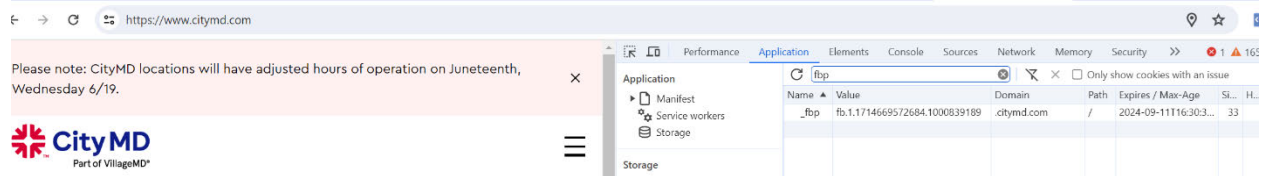


Figure 15. screenshot showing defendant's use of a first party `_fbp` cookie.

99. The Pixel uses both first- and third-party cookies, and both were used on the Website.²⁸

100. At present, the full breadth of Defendant's tracking and data sharing practices is unclear, but evidence suggests Defendant is using additional tracking pixels and tools to transmit its patients' Private Information to additional third parties. For example, the image below indicates that Defendant is also sending its patients' protected health information to Google via Google Analytics:

²⁷ Defendant's Website tracks and transmits data via first-party and third-party cookies. The `c_user` cookie or Facebook ID is a type of third-party cookie assigned to each person who has a Facebook account, and it is comprised by a unique and persistent set of numbers.

²⁸ A first-party cookie is "created by the website the user is visiting"—in this case, Defendant's Website. A third-party cookie is "created by a website with a domain name other than the one the user is currently visiting"—i.e., Facebook. The `_fbp` cookie is always transmitted as a first-party cookie. At a minimum, Facebook uses the `fr`, `_fbp`, and `c_user` cookies to link website visitors' data to their Facebook IDs and corresponding accounts.

²⁹ See *Google Analytics Dev Tools: Measurement Protocol Reference: Required Values for All Hits*, <https://developers.google.com/analytics/devguides/collection/protocol/v1/reference> (last visited May 23, 2024).

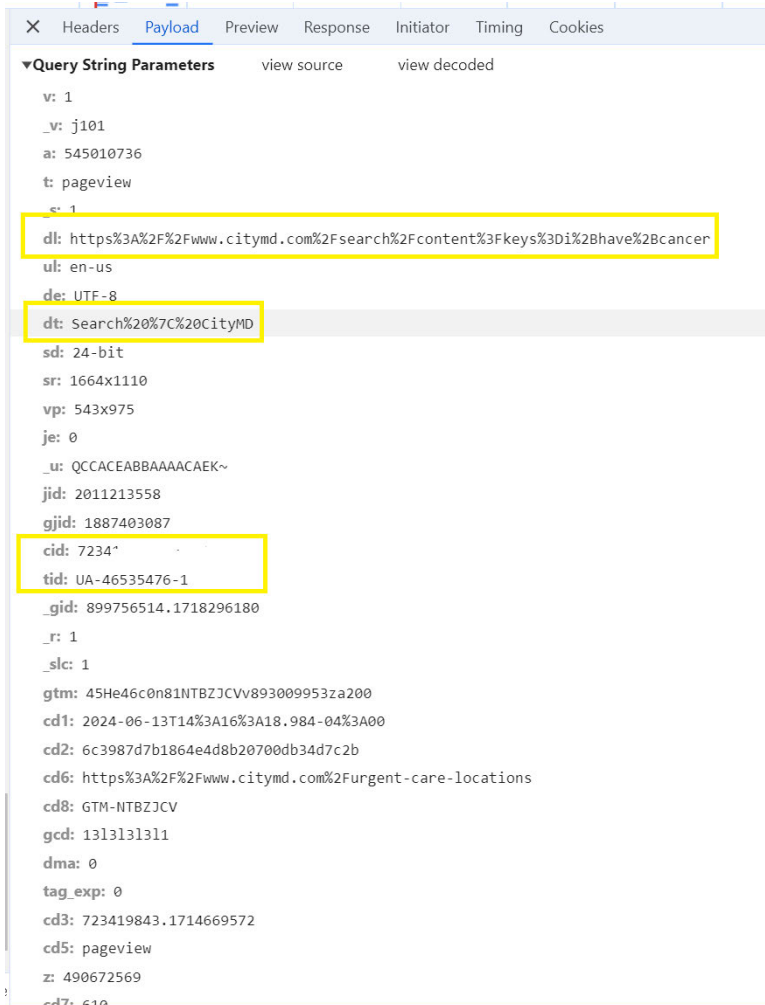


Figure 17. screenshot of Google Analytics Payload, depicting the Defendant's unique identifier ("tid= UA-465e35476-1"), the user's unique identifier ("cid"),³⁰ and the specific search the user made on the Website.

101. The images above contain the user's search phrase ("I have cancer"), and Defendant does not appear to have enabled the anonymize feature provided by Google Analytics because the text "aip:" does not appear in the image, thereby revealing the user's status as a patient and that the patient is seeking treatment for cancer.

102. Accordingly, Google receives patients' communications alongside the patients' IP address, which is also personally identifiable and impermissible under HIPAA.

³⁰ The *cid* has been redacted to protect the user's identity.

103. Defendant does not disclose that the Pixels, Google Analytics, or any other Tracking Technologies embedded in the Website’s source code track, record, and transmit Plaintiff’s and Class Members’ Private Information to Facebook and Google. Moreover, Defendant never received consent or written authorization to disclose Plaintiff’s and Class Members’ private communications to Facebook or Google.

G. Defendant’s Conduct Is Unlawful and Violated Industry Norms.

i. Defendant Violated its own Privacy Policy.

104. Defendant’s Website Privacy Policy states, “[w]hen you browse our website, you do so anonymously, unless you have previously indicated that you wish CityMD to remember your login and password or you submit a registration form. We do not collect personal information for the purpose of reselling or distributing that information.”³¹

105. Defendant’s Privacy Policy is clear that CityMD “will require your affirmative action to indicate your consent before we use your information for purposes other than the purpose for which it was submitted.”³²

106. Defendant’s Privacy Policy further promises that “[y]our personal information is never shared outside CityMD without your permission, except under conditions explained below.” Those conditions – none of which apply here – include sharing updates on new products, sharing news about software updates, and where it is required by law.³³

³¹ See <https://www.citymd.com/privacy> (“Personal information means any information that may be used to identify an individual, including, but not limited to, a first and last name, email address, a home, postal or other physical address, other contact information, title, birth date, gender, occupation, industry, personal interests, medical conditions or other information when needed to provide a service you requested.”) (last visited Jun. 13, 2024).

³² *Id.*

³³ *Id.*

107. Defendant violated its own Privacy Policy by unlawfully disclosing Plaintiff's and Class Members' Private Information to Meta (Facebook), Google, and likely other third parties without written authorization.

108. Protected health information is further governed by Defendant's Notice of Privacy Practices.

109. Defendant's Notice of Privacy Practices explicitly explains "[h]ow medical information about you may be used and disclosed."³⁴ In this Notice, Defendant expressly maintains that "[u]ses and disclosures [of PHI] for marketing purposes" are to "be made only with your authorization."

110. At no point did CityMD seek such authorization from Plaintiff before transmitting protected health information to a third party for marketing purposes.

111. Defendant's Notice of Privacy Practices further allows that "[y]ou have the right to request a restriction of your protected health information."³⁵ This language reflects Defendant's awareness of the high value patients such as Plaintiff and Class Members place on their protected health information.

112. Defendant's transmission of protected health information to third parties such as Facebook or Google violated its own Notice of Privacy Practices, in which CityMD acknowledges that "[w]e are required to abide by the terms of this Notice of Privacy Practices."³⁶

³⁴ See Notice of Privacy Practices (last updated February 1, 2019), <https://www.citymd.com/sites/default/files/2022-06/citymd-nj-ny-npp-2022.pdf> (last visited Jun. 13, 2024).

³⁵ *Id.*

³⁶ *Id.*

ii. Defendant Violated HIPAA Standards.

113. Under HIPAA, a healthcare provider may not disclose personally identifiable, non-public medical information about a patient, a potential patient or household member of a patient for marketing purposes without the patients' express written authorization.³⁷

114. The HIPAA Privacy Rule “establishes national standards to protect individuals’ medical records and other individually identifiable health information (collectively defined as ‘protected health information’) and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically.”³⁸

115. The Privacy Rule broadly defines “protected health information” (“PHI”) as individually identifiable health information (“IIHI”) that is “transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium.” 45 C.F.R. § 160.103.

116. IIHI is defined as “a subset of health information, including demographic information collected from an individual” that is: (1) “created or received by a health care provider, health plan, employer, or health care clearinghouse”; (2) “[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual”; and (3) either (a) “identifies the individual” or (b) “[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual.” 45 C.F.R. § 160.103.

117. Under the HIPAA de-identification rule, “health information is not individually identifiable only if”: (1) an expert “determines that the risk is very small that the information could

³⁷ HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).

³⁸ *HIPAA For Professionals*, <https://www.hhs.gov/hipaa/for-professionals/index.html> (last visited Jun. 7, 2024).

be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information” and “documents the methods and results of the analysis that justify such determination”; or (2) “the following identifiers of the individual or of relatives, employers, or household members of the individual are removed;

A. Names;

H. Medical record numbers;

J. Account numbers;

M. Device identifiers and serial numbers;

N. Web Universal Resource Locators (URLs);

O. Internet Protocol (IP) address numbers; ... and

R. Any other unique identifying number, characteristic, or code...; and”

The covered entity must not “have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.”

45 C.F.R. § 160.514.

118. The HIPAA Privacy Rule requires any “covered entity”—which includes health care providers—to maintain appropriate safeguards to protect the privacy of protected health information and sets limits and conditions on the uses and disclosures that may be made of protected health information without authorization. 45 C.F.R. §§ 160.103, 164.502.

119. An individual or corporation violates the HIPAA Privacy Rule if it knowingly and in violation of 42 U.S.C. §§ 1320d-1320d-9 (“Part C”): “(1) uses or causes to be used a unique health identifier; [or] (2) obtains individually identifiable health information relating to an individual.” The statute states that a “person ... shall be considered to have obtained or disclosed individually identifiable health information in violation of [Part C] if the information is maintained

by a covered entity ... and the individual obtained or disclosed such information without authorization.” 42 U.S.C. § 1320d-6.

120. The criminal and civil penalties imposed by 42 U.S.C. § 1320d-6 apply directly to Defendant when it is knowingly disclosing individually identifiable health information relating to an individual, as those terms are defined under HIPAA.

121. Violation of 42 U.S.C. § 1320d-6 is subject to criminal penalties. 42 U.S.C. § 1320d-6(b). There is a penalty enhancement where “the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm.” In such cases, the entity that knowingly obtains individually identifiable health information relating to an individual shall “be fined not more than \$250,000, imprisoned not more than 10 years, or both.”

122. In its *Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act Privacy Rule*, the HHS instructs:

Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data... If such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.³⁹

123. In its guidance for marketing, HHS further instructs:

The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual’s written authorization before a use or

³⁹https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf (last visited June 7, 2024).

disclosure of his or her protected health information can be made for marketing. ... Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, *covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list.* (emphasis added).⁴⁰

124. As described above, the OCR addresses the obligations of “regulated entities,” which are HIPAA-covered entities and business associates, when using tracking technologies.⁴¹

125. The Bulletin expressly provides that “[r]egulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules.” (emphasis in original).

126. As such, Defendant's actions violated HIPAA.

iii. Defendant Violated Industry Standards.

127. A medical provider's duty of confidentiality is a cardinal rule and is embedded in the physician-patient and hospital-patient relationship.

128. The American Medical Association's (“AMA”) Code of Medical Ethics contains numerous rules protecting the privacy of patient data and communications.

129. AMA Code of Ethics Opinion 3.1.1 provides:

Protecting information gathered in association with the care of the patient is a core value in health care... Patient privacy encompasses a number of aspects, including, ... personal data (informational privacy)

130. AMA Code of Medical Ethics Opinion 3.2.4 provides:

⁴⁰<https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf> (last visited Jun. 7, 2024).

⁴¹ See OCR Bulletin *supra*, note 7.

Information gathered and recorded in association with the care of the patient is confidential. Patients are entitled to expect that the sensitive personal information they divulge will be used solely to enable their physician to most effectively provide needed services. Disclosing information for commercial purposes without consent undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient-physician relationship. Physicians who propose to permit third-party access to specific patient information for commercial purposes should: (A) Only provide data that has been de-identified. [and] (b) Fully inform each patient whose record would be involved (or the patient's authorized surrogate when the individual lacks decision-making capacity about the purposes for which access would be granted.

131. AMA Code of Medical Ethics Opinion 3.3.2 provides:

Information gathered and recorded in association with the care of a patient is confidential, regardless of the form in which it is collected or stored. Physicians who collect or store patient information electronically...must...(c) release patient information only in keeping ethics guidelines for confidentiality.

H. Plaintiff's and Class Members' Reasonable Expectation of Privacy.

132. Plaintiff and Class Members were aware of Defendant's duty of confidentiality when they sought medical services from Defendant.

133. Indeed, at all times when Plaintiff and Class Members provided their Private Information to Defendant, they each had a reasonable expectation that the information would remain private and that Defendant would not share the Private Information with third parties for a commercial purpose, unrelated to patient care.

134. Privacy polls and studies show that the overwhelming majority of Americans consider obtaining an individual's affirmative consent before a company collects and shares its customers' data to be one of the most important privacy rights.

135. For example, a Consumer Reports study shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing

consumer data, and the same percentage believe those companies and websites should be required to provide consumers with a complete list of the data that is collected about them.⁴²

136. Personal data privacy and obtaining consent to share Private Information are material to Plaintiff and Class Members.

137. Plaintiff and Class Members would not have used Defendant's Website, would not have provided their Private Information to Defendant and would not have paid for Defendant's healthcare services or would have paid less for them, had they known that Defendant would disclose their Private Information to third parties.

138. Plaintiff's and Class Members' reasonable expectations of privacy in their PII/PHI are grounded in, among other things, Defendant's status as a healthcare provider, Defendant's common law obligation to maintain the confidentiality of patients' PII/PHI, state and federal laws protecting the confidentiality of medical information, state and federal laws protecting the confidentiality of communications and computer data, state laws prohibiting the unauthorized use and disclosure of personal means of identification and Defendant's express and implied promises of confidentiality.

I. IP Addresses Are PII.

139. In addition to patient status, medical treatment and patients' unique Facebook ID, Defendant improperly disclosed and otherwise assisted Facebook, Google and/or other third parties with intercepting Plaintiff's and Class Members' Computer IP addresses.

140. An IP address is a number that identifies the address of a device connected to the Internet.

⁴² *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, (May 11, 2017), <https://www.consumerreports.org/consumer-reports/consumers-lessconfident-about-healthcare-data-privacy-and-car-safety-a3980496907/> (last visited June 4, 2024).

141. IP addresses are used to identify and route communications on the Internet.

142. IP addresses of individual Internet users are used by Internet service providers, websites, and third-party tracking companies to facilitate and track Internet communications.

143. Facebook tracks every IP address ever associated with a Facebook user, and uses that information for targeting individual homes and their occupants with advertising.

144. As to Google, over 70% of online websites use Google's visitor-tracking products, Google Analytics and Google Ad Manager.

145. Whenever a user visits a website that is running Google Analytics and Google Ad Manager, Google's software scripts on the website surreptitiously direct the user's browser to send a secret, separate message to Google's servers in California, which includes the user's IP address, the user's geolocation, information contained in Google cookies, any user-ID issued by the website to the user, and information about the browser the user is using.

146. Under HIPAA, an IP address is considered PII.⁴³

147. HIPAA defines PII to include "any unique identifying number, characteristic or code" and specifically lists the example of IP addresses.⁴⁴

148. HIPAA further declares information as personally identifiable where the covered entity has "actual knowledge that the information to identify an individual who is a subject of the information."⁴⁵

149. Consequently, by disclosing IP addresses, Defendant's business practices violated HIPAA and industry privacy standards.

⁴³ HIPAA defines PII to include "any unique identifying number, characteristic or code" and specifically lists the example of IP addresses. *See* 45 C.F.R. § 164.514 (2).

⁴⁴ *See* 45 C.F.R. § 164.514(2).

⁴⁵ 45 C.F.R. § 164.514(2)(ii); *see also* 45 C.F.R. § 164.514(b)(2)(i)(O).

J. CityMD Was Enriched and Benefitted from the Use of the Tracking Technologies and Unauthorized Disclosures.

150. One of the primary reasons that Defendant decided to embed the Pixel and other tracking technologies on its Website was to commit criminal and tortious acts in violation of federal and state laws as alleged herein, namely, the use of patient data in the absence of express written consent.

151. Defendant's disclosure of the Private Information after the initial interception, including for for marketing and revenue generation, was in violation of HIPAA and an invasion of privacy.

152. In exchange for disclosing the Private Information of its patients, Defendant is compensated by Facebook and Google in the form of enhanced advertising services and more cost-efficient marketing.

153. Retargeting is a form of online marketing that targets users with ads based on their previous internet communications and interactions.

154. The process of increasing conversions and retargeting occurs in the healthcare context by sending a successful action on a health care website back to Facebook via the Tracking Technologies and the Pixel embedded on, in this case, Defendant's Website.

155. For example, when a user searches for an urgent care location on the Website, that information is sent to Facebook. Facebook can then use its data on the user to find more users to click on a CityMD ad and ensure that the users targeted are more likely to convert.⁴⁶

⁴⁶ See *How to Make Facebook Ads HIPAA Compliant and Still Get Conversion Tracking* (Mar. 14, 2023), <https://www.freshpaint.io/blog/how-to-make-facebook-ads-hipaa-compliantand-still-get-conversion-tracking> (last accessed June 6, 2024).

156. Through this process, the Pixel loads and captures as much data as possible when a user loads a telehealth website that has installed the Pixel. The information the Pixel captures, “includes URL names of pages visited, and actions taken—all of which could be potential examples of health information.”⁴⁷

157. As part of its marketing campaign, Defendant re-targeted patients and potential patients to get more visitors to its Website to use its services. Defendant did so through use of the intercepted patient data it obtained, procured and/or disclosed in the absence of express written consent.

158. Companies have started to warn about the potential HIPAA violations associated with using pixels and tracking technologies because many such trackers are not HIPAA-compliant or are only HIPAA-compliant if certain steps are taken.⁴⁸

159. For example, Freshpaint, a healthcare marketing vendor, cautioned that “Meta isn’t HIPAA-compliant. They don’t sign BAAs, and the Meta Pixel acts like a giant personal user data vacuum sending PHI to Meta servers,” and “[i]f you followed the Facebook (or other general) documentation to set up your ads and conversion tracking using the Meta Pixel, remove the Pixel now.”⁴⁹

⁴⁷ <https://www.freshpaint.io/blog/how-to-make-facebook-ads-hipaa-compliant-and-still-get-conversion-tracking#:~:text=When%20a%20Facebook%20user%20clicks,potential%20examples%20of%20health%20information>.

⁴⁸ See *The guide to HIPAA compliance in analytics*, <https://campaign.piwik.pro/wpcontent/uploads/2023/10/The-guide-to-HIPAA-compliance-in-analytics.pdf> (explaining that Google Analytics 4 is not HIPAA-compliant) (last accessed June 4, 2024).

⁴⁹ *How To Make Facebook Ads HIPAA Compliant and Still Get Conversion Tracking*, *supra* note 46.

160. Medico Digital also warns that “retargeting requires sensitivity, logic and intricate handling. When done well, it can be a highly effective digital marketing tool. But when done badly, it could have serious consequences.”⁵⁰

161. By utilizing the Tracking Technologies, the cost of advertising and retargeting was reduced through further use of the unlawfully intercepted and disclosed Private Information, thereby benefitting Defendant while invading the privacy of Plaintiff and Class Members and violating their rights under federal and Arizona law.

K. Plaintiff’s and Class Members’ Private Information Had Financial Value.

162. Plaintiff’s Private Information has economic value and Defendant’s disclosures harmed Plaintiff and Class Members.

163. Facebook regularly uses the data that it acquires to create Core and Custom Audiences as well as Lookalike Audiences and then sells that information to advertising clients.

164. Plaintiff’s and Class Members’ Private Information has considerable value as highly monetizable data especially insofar as it allows companies to gain insight into their customers so that they can perform targeted advertising and boost their revenues.

165. Professor Paul M. Schwartz, writing in the Harvard Law Review, notes: “Personal information is an important currency in the new millennium. The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from the trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information.”⁵¹

⁵⁰ The complex world of healthcare retargeting (July 10, 2023), <https://www.medicodigital.com/the-complicated-world-of-healthcare-retargeting> (last accessed June 4, 2024).

⁵¹ Paul M. Schwartz, Property, Privacy, and Personal Data, 117 Harv. L. Rev. 2055, 2056-57 (2004).

166. Various reports have been conducted to identify the value of health data. For example, in 2023, the Value Examiner published a report entitled Valuing Healthcare Data. The report focused on the rise in providers, software firms and other companies that are increasingly seeking to acquire clinical patient data from healthcare organizations. The report cautioned providers that they must de-identify data and that purchasers and sellers of “such data should ensure it is priced at fair market value to mitigate any regulatory risk.”⁵²

167. Trustwave Global Security also published a report entitled The Value of Data. With respect to healthcare data records, the report found that they may be valued at up to \$250 per record on the black market, compared to \$5.40 for the next highest value record (a payment card).⁵³

168. The value of health data has also been reported extensively in the media. For example, CNBC published an article in 2019 in which it observed that “[d]e-identified patient data has become its own small economy: There’s a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers.”⁵⁴

169. Similarly, Time Magazine published an article in 2017 titled “How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry” in which it described the extensive market for health data and observed that the market for information was both lucrative and a significant risk to privacy.⁵⁵

⁵² See

<https://www.healthcapital.com/researchmaterialdocuments/publishedarticles/Valuing%20Healthcare%20Data.pdf> (last visited June 5, 2024).

⁵³ See <https://www.imprivata.com/blog/healthcare-data-new-prize-hackers> (citing https://www.infopoint-security.de/media/TrustwaveValue_of_Data_Report_Final_PDF.pdf) (last visited June 4, 2024).

⁵⁴ See <https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html> (last visited June 7, 2024).

⁵⁵ See <https://time.com/4588104/medical-data-industry/> (last visited June 7, 2024)

170. Indeed, numerous marketing services and consultants offering advice to companies on how to build their email and mobile phone lists—including those seeking to take advantage of targeted marketing—direct putative advertisers to offer consumers something of value in exchange for their personal information. “No one is giving away their email address for free. Be prepared to offer a book, guide, webinar, course or something else valuable.”⁵⁶

171. There is also a market for data in which consumers can participate. Personal information has been recognized by courts as extremely valuable. *See, e.g., In re Marriott Int’l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D. Md. 2020) (“Neither should the Court ignore what common sense compels it to acknowledge—the value that personal identifying information has in our increasingly digital economy. Many companies, like Marriott, collect personal information. Consumers too recognize the value of their personal information and offer it in exchange for goods and services.”).

172. This economic value has been leveraged largely by corporations who pioneered the methods of its extraction, analysis and use. However, the data also has economic value to Internet users. Market exchanges have sprung up where individual users like Plaintiff herein can sell or monetize their own data.

173. Several companies, such as Google, Nielsen, UpVoice, HoneyGain and SavvyConnect, have products through which they pay consumers for a license to track their data.⁵⁷

174. Facebook has also paid users for their digital information, including browsing history. Until 2019, Facebook ran a “Facebook Research” app through which it paid \$20 a month

⁵⁶ VERO, HOW TO COLLECT EMAILS ADDRESSES ON TWITTER <https://www.getvero.com/resources/twitter-lead-generation-cards/> (last visited June 7, 2024).

⁵⁷ *See 10 Apps for Selling Your Data for Cash*, <https://wallethacks.com/apps-for-selling-your-data/> (last accessed June 5, 2024).

for a license to collect browsing history information and other communications from consumers between the ages 13 and 35.

175. Additionally, healthcare data is extremely valuable to bad actors. Health care records may be valued at up to \$250 per record on the black market.⁵⁸

176. These rates are assumed to be discounted because they do not operate in competitive markets, but rather, in an illegal marketplace. If a criminal can sell other Internet users' stolen data, surely Internet users can sell their own data.

177. Healthcare data is incredibly valuable because, unlike a stolen credit card that can be easily canceled, most people are unaware that their medical information has been sold. Once it has been detected, it can take years to undo the damage caused.

178. In short, there is a quantifiable economic value to Internet users' data that is greater than zero. The exact number will be a matter for experts to determine.

179. Defendant gave away Plaintiff's and Class Members' communications and transactions on its Website without permission.

180. The unauthorized access to Plaintiff's and Class Members' personal and Private Information has diminished the value of that information, resulting in harm to Website users, including Plaintiff and Class Members.

PLAINTIFF ANDRETTA'S EXPERIENCE

181. As a condition of receiving Defendant's services, Plaintiff Andretta disclosed her Private Information to Defendant on numerous occasions, and most recently around October 2021.

182. Plaintiff Andretta accessed Defendant's Website on her phone and computer to research and provide information regarding the healthcare services she received from Defendant.

⁵⁸ Tori Taylor, *Hackers, Breaches, and the Value of Healthcare Data*, *SecureLink* (June 30, 2021), <https://www.imprivata.com/blog/healthcare-data-new-prize-hackers> (last accessed June 7, 2024).

183. Plaintiff Andretta used Defendant's services to request and book doctor's appointments for herself as well as review her medical records and access Defendant's patient portal.

184. During the relevant time period, Plaintiff Andretta used Defendant's Website to research symptoms, testing, and diagnosis for both Covid-19 and the flu and other sensitive health conditions and to search for Defendant's locations close to her address. Her searches for information related to [REDACTED] included her visiting specific webpages that revealed her PHI through the URLs as well as searches through the Website's search bar that disclosed the specific phrases she used to search for information related to her medical conditions.

185. The full scope of Defendant's interceptions and disclosures of Plaintiff's communications to Meta can only be determined through formal discovery. However, in addition to disclosing the specific searches Plaintiff entered into the Website's search bar, Defendant intercepted at least the following communications about Plaintiff's patient status, medical conditions (including her treatment and diagnosis of [REDACTED]), treatments sought, and the locations for receipt of healthcare, via the following long-URLs or substantially similar URLs that were sent to Meta via the Pixel (and which contain information concerning Plaintiff's specific medical conditions, queries, and treatments sought:

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

186. Plaintiff Andretta has used and continues to use the same devices to maintain and access an active Facebook account throughout the relevant period in this case.

187. Plaintiff Andretta reasonably expected that her communications with Defendant via the Website were confidential, solely between herself and Defendant, and that such communications would not be transmitted to or intercepted by a third party.

188. However, as a result of the Tracking Technologies Defendant chose to install on its Website, Plaintiff Andretta's Private Information was intercepted, viewed, analyzed and used by unauthorized third parties.

189. Defendant transmitted Plaintiff Andretta's Facebook ID, computer IP address and other device and unique online identifiers to Facebook. Defendant also transmitted information such as health and medical information including Plaintiff's particular health condition, the type of medical treatment sought, patient status and the fact that Plaintiff attempted to or did book a medical appointment.

190. Plaintiff Andretta never consented to the disclosure of or use of her Private Information by third parties or to Defendant enabling third parties, including Facebook, to access or interpret such information. Plaintiff Andretta never consented to any third parties' receipt or use of her Private Information.

191. Notwithstanding, through the Tracking Technologies embedded on Defendant's Website, Defendant transmitted Plaintiff Andretta's Private Information to, at a minimum, Facebook and likely many other third parties like Google, Bing and others.

192. As a result, Plaintiff Andretta received targeted ads on Facebook or Instagram inviting her to visit other CityMD urgent care locations, even after she had made use of their services, as well as ads related [REDACTED]

193. By making these disclosures without her consent, Defendant breached Plaintiff Andretta's privacy and unlawfully disclosed her Private Information.

194. Defendant did not inform Plaintiff Andretta that it had shared her Private Information with Facebook.

195. Plaintiff Andretta used and continues to use the same devices to maintain and to access an active Facebook account throughout the relevant period for this case.

196. Plaintiff Andretta has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future unauthorized disclosure(s).

TOLLING

197. Any applicable statute of limitations has been tolled by the "delayed discovery" rule. Plaintiff did not know (and had no way of knowing) that their PII and/or PHI was intercepted and unlawfully disclosed to Facebook, Google and potentially other third parties because Defendant kept this information secret. Alternatively, applicable statute of limitations have been tolled by other applicable rules or doctrines.

CLASS ACTION ALLEGATIONS

198. Plaintiff Andretta brings this action on behalf of herself and on behalf of all other persons similarly situated ("the Class") pursuant to Rule 23(b)(2), 23(b)(3) and 23(c)(4) of the Federal Rules of Civil Procedure.

199. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

All individuals residing in the United States whose Private Information was disclosed to a third party without authorization or consent through the Meta Pixel and other tracking technologies on CityMD's Website.

200. The New York Sub-Class that Plaintiff seeks to represent is defined as:

All individuals residing in the State of New York whose Private Information was disclosed to a third party without authorization or consent through the Meta Pixel and other tracking technologies on CityMD's Website.

201. The Nationwide Class and New York Sub-Class are collectively referred to as the "Class" unless otherwise and more specifically identified.

202. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

203. Plaintiff reserves the right to modify or amend the definition of the proposed class before the Court determines whether certification is appropriate.

204. Numerosity, Fed R. Civ. P. 23(a)(1). The Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are hundreds of thousands of individuals whose PII and PHI may have been improperly disclosed to Facebook, and the Class is identifiable within Defendant's records.

205. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3). Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

- a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiff and Class Members;
- b. Whether Defendant had duties not to disclose the Private Information of Plaintiff and Class Members to unauthorized third parties;

- c. Whether Defendant adequately, promptly and accurately informed Plaintiff and Class Members that their Private Information would be disclosed to third parties;
- d. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their Private Information had been compromised;
- e. Whether Defendant adequately addressed and fixed the practices which permitted the disclosure of patient Private Information;
- f. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiff and Class Members;
- g. Whether Plaintiff and Class Members are entitled to actual, consequential and/or nominal damages as a result of Defendant's wrongful conduct; and
- h. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of Defendant's disclosure of their Private Information.

206. Typicality, Fed. R. Civ. P. 23(a)(3). Plaintiff's claims are typical of those of other Class Members because all had their Private Information compromised as a result of Defendant's incorporation of the tracking technologies, due to Defendant's misfeasance.

207. Adequacy, Fed. R. Civ. P. 23(a)(4). Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. Plaintiff has also retained

counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

208. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3). Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against a large corporation like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

209. Policies Generally Applicable to the Class. Fed. R. Civ. P. 23(b)(2). This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

210. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would

necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

211. The litigation of the claims is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

212. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

213. Unless a class-wide injunction is issued, Defendant may continue disclosing the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the practices complained of herein, and Defendant may continue to act unlawfully as set forth in this Complaint.

214. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

215. Issue Certification, Fed. R. Civ. P. 23(c)(4). Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the

resolution of which would advance the disposition of this matter and the parties' interests therein.

Such particular issues include, but are not limited to, the following:

- a. Whether Defendant owed a legal duty to not disclose Plaintiff's and Class Members' Private Information;
- b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;
- c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;
- d. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their Private Information would be disclosed to third parties;
- e. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information disclosed to third parties;
- f. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

CAUSES OF ACTION

COUNT I

VIOLATIONS OF ELECTRONIC COMMUNICATIONS PRIVACY ACT

18 U.S.C. § 2511(1), *et seq.*

UNAUTHORIZED INTERCEPTION, USE AND DISCLOSURE

(On Behalf of Plaintiff & the Nationwide Class)

216. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

217. The ECPA prohibits the intentional interception of the content of any electronic communication. 18 U.S.C. § 2511.

218. The ECPA protects both sending and receipt of communications.

219. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

220. The transmissions of Plaintiff's Private Information to Defendant via Defendant's Website qualifies as a "communication" under the ECPA's definition in 18 U.S.C. § 2510(12).

221. The transmissions of Plaintiff's Private Information to medical professionals qualifies as a "communication" under the ECPA's definition in 18 U.S.C. § 2510(2).

222. **Electronic Communications.** The transmission of Private Information between Plaintiff and Class Members and Defendant via its Website with which they chose to exchange communications are "transfer[s] of signs, signals, writing,...data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(2).

223. **Content.** The ECPA defines content, when used with respect to electronic communications, to "include[] *any* information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8) (emphasis added).

224. **Interception.** The ECPA defines the interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device" and "contents ... include any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(4), (8).

225. **Electronic, Mechanical, or Other Device.** The ECPA defines “electronic, mechanical, or other device” as “any device ... which can be used to intercept a[n] ... electronic communication[.]” 18 U.S.C. § 2510(5).

226. The following constitute “devices” within the meaning of 18 U.S.C. § 2510(5):

- a. The cookies Defendant and third parties, such as Meta and Google, use to track Plaintiff’s and Class Members’ communications;
- b. Plaintiff’s and Class Members’ browsers;
- c. Plaintiff’s and Class Members’ computing devices;
- d. Defendant’s web-servers and
- e. The Tracking Technologies deployed by Defendant to effectuate the sending and acquisition of patient communications.

227. Whenever Plaintiff and Class Members interacted with Defendant’s Website, Defendant, through the Tracking Technologies embedded and operating on its Website, contemporaneously and intentionally disclosed, and endeavored to disclose the contents of Plaintiff’s and Class Members’ electronic communications to third parties, including Facebook and Google, without authorization or consent, and knowing or having reason to know that the electronic communications were obtained in violation of the ECPA. 18 U.S.C. § 2511(1)(c).

228. Whenever Plaintiff and Class Members interacted with Defendant’s Website, Defendant, through the Tracking Technologies embedded and operating on its Website, contemporaneously and intentionally used, and endeavored to use the contents of Plaintiff’s and Class Members’ electronic communications, for purposes other than providing health care services to Plaintiff and Class Members without authorization or consent, and knowing or having reason to

know that the electronic communications were obtained in violation of the ECPA. 18 U.S.C. § 2511(1)(d).

229. Whenever Plaintiff and Class Members interacted with Defendant's Website, Defendant, through the Tracking Technologies it embedded, configured and operated on its Website, contemporaneously and intentionally disclosed the contents of Plaintiff's and Class Members' electronic communications while those communications were in transmission, to persons or entities other than an addressee or intended recipient of such communication, including Facebook and Google.

230. Defendant's intercepted communications include, but are not limited to, the contents of communications to and/or from Plaintiff's and Class Members' regarding PII and PHI, treatment, scheduling details and bill payments.

231. Additionally, through the above-described Tracking Technologies and intercepted communications, this information was, in turn, used by third parties, such as Facebook, to 1) place Plaintiff in specific health-related categories and 2) target Plaintiff with advertising associated with Plaintiff's specific health conditions.

232. By intentionally disclosing or endeavoring to disclose the electronic communications of Plaintiff and Class Members to affiliates and other third parties, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

233. By intentionally using, or endeavoring to use, the contents of the electronic communications of Plaintiff and Class Members, while knowing or having reason to know that the

information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

234. Defendant intentionally used the wire or electronic communications to increase its profit margins. Defendant specifically used the Tracking Technologies to track and utilize Plaintiff's and Class Members' PII and PHI for financial gain.

235. Defendant was not acting under color of law to intercept and disclose Plaintiff's and Class Members' wire or electronic communication.

236. Plaintiff and Class Members did not authorize Defendant to acquire the content of their communications for purposes of disclosing those communications to third parties in violation of HIPAA and invading Plaintiff's privacy via the Tracking Technologies.

237. Any purported consent that Defendant received from Plaintiff and Class Members was not valid.

238. **Unauthorized Purpose.** Defendant intentionally intercepted the contents of Plaintiff's and Class Members' electronic communications for the purpose of committing a tortious or criminal act in violation of the Constitution or laws of the United States or of any State, such as New York—namely, to disclose that interception in violation of HIPAA and invasion of privacy, among others.

239. **Any party exception in 18 U.S.C. § 2511(2)(d) does not apply.** The party exception in § 2511(2)(d) does not permit a party that intercepts or causes interception to escape liability if the communication is intercepted for the purpose of committing any tortious or criminal act in violation of the Constitution or laws of the United States or of any State.

240. Defendant is a “party to the communication” with respect to patient communications. However, Defendant's simultaneous, unknown duplication, forwarding and

disclosure of Plaintiff's and Class Members' Private Information does not qualify for the party exemption.

241. Here, as alleged above, Defendant violated a provision of the Health Insurance Portability and Accountability Act, specifically 42 U.S.C. § 1320d-6(a)(3). This provision imposes a criminal penalty for knowingly disclosing individually identifiable health information (IIHI) to a third party. HIPAA defines IIHI as:

any information, including demographic information collected from an individual, that—(A) is created or received by a health care provider ... (B) *relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual*, and (i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.⁵⁹

242. Plaintiff's information that Defendant disclosed to third parties qualifies as IIHI, and Defendant violated Plaintiff's expectations of privacy, and constitutes tortious and/or criminal conduct through a violation of 42 U.S.C. § 1320d(6). Defendant used the wire or electronic communications to increase its profit margins. Defendant specifically used the tracking technologies to track and utilize Plaintiff's and Class Members' PII and PHI for financial gain.

243. The penalty for violation is enhanced where “the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm.” 42 U.S.C. § 1320d-6.

244. Defendant's conduct violated 42 U.S.C. § 1320d-6 in that it:

- a. Used and caused to be used cookie identifiers associated with specific patients without patient authorization; and

⁵⁹ § 1320d-(6) (emphasis added).

b. Disclosed IIIHI to Facebook and Google without patient authorization.

245. Defendant's conduct would be subject to the enhanced provisions of 42 U.S.C. § 1320d-6 because Defendant's use of the Facebook and Google source code was for Defendant's commercial advantage to increase revenue from existing patients and gain new patients.

246. Healthcare patients have the right to rely upon the promises that companies make to them. Defendant accomplished its tracking and retargeting through deceit and disregard, such that an actionable claim may be made, in that it was accomplished through source code that cause Facebook pixels and cookies (including but not limited to the fbp, ga and gid cookies) and other tracking technologies to be deposited on Plaintiff's and Class members' computing devices as "first-party" cookies that are not blocked.

247. The _fbp, ga, and cid cookies, commanded Plaintiff's and Class Members' computing devices to redirect and disclose their data and the content of their communications with Defendant to Google, Facebook, and others.

248. Defendant knew or had reason to know that the fbp, ga, and gid cookies would command Plaintiff's and Class Members' computing devices to remove, redirect and disclose their data and the content of their communications with Defendant to Google, Facebook, and others.

249. Defendant's scheme or artifice to defraud in this action consists of: (a) the false and misleading statements and omissions in its privacy policy (HIPAA Notice) set forth above, including the statements and omissions recited in the claims below and (b) the placement of the 'fbp,' "ga," and "gid," cookies on patient computing devices disguised as a first-party cookie on Defendant's Website rather than a third-party cookie from Meta.

250. Defendant acted with the intent to defraud in that it willfully invaded and took Plaintiff's and Class Members' property rights (a) to the confidentiality of Private Information and

their right to determine whether such information remains confidential and exclusive right to determine who may collect and/or use such information for marketing purposes and (b) to determine who has access to their computing devices.

251. As such, Defendants cannot viably claim any exception to ECPA liability.

252. Plaintiff and Class Members have suffered damages as a direct and proximate result of Defendant's invasion of privacy in that:

- a. Learning that Defendant has intruded upon, intercepted, transmitted, shared, and used their individually identifiable patient health information (including information about their medical symptoms, conditions, treatments and concerns, medical appointments, healthcare providers and locations, health insurance and medical bills) for commercial purposes has caused Plaintiff and the Class Members to suffer emotional distress;
- b. Defendant received substantial financial benefits from its use of Plaintiff's and Class Members' PII and/or PHI without providing any value or benefit to Plaintiff or the Class Members;
- c. Defendant received substantial, quantifiable value from its use of Plaintiff's and Class Members' PII and/or PHI, such as understanding how people use its website and determining what ads people see on its website, without providing any value or benefit to Plaintiff or the Class Members;
- d. Defendant has failed to provide Plaintiff and the Class Members with the full value of the medical services for which they paid, which included a duty to maintain the confidentiality of their patient information; and

- e. The diminution in value of Plaintiff's and Class Members' PII and PHI and the loss of privacy due to Defendant making sensitive and confidential information, such as patient status, test results, and appointments that Plaintiff and Class Members intended to remain private no longer private.

253. As a result of Defendant's violation of the ECPA, Plaintiff and Class Members are entitled to all damages available under 18 U.S.C. § 2520, including statutory damages of whichever is the greater of \$100 a day for each day of violation or \$10,000, equitable or declaratory relief, compensatory and punitive damages, and attorney's fees and costs.

COUNT II
BREACH OF IMPLIED CONTRACT
(on behalf of Plaintiff & the Nationwide Class)

254. Plaintiff repeats and re-alleges every allegation contained in the Complaint as if fully set forth herein.

255. As a condition of utilizing Defendant's Website and receiving services from Defendant's healthcare facilities and professionals, Plaintiff and the Class Members provided their Private Information and compensation for their medical care.

256. When Plaintiff and Class Members provided their Private Information to Defendant, they entered an implied contract pursuant to which Defendant agreed to safeguard and not disclose their Private Information without consent.

257. Plaintiff and Class Members would not have entrusted Defendant with their Private Information in the absence of an implied contract between them and Defendant obligating Defendant to not disclose Private Information without consent.

258. Plaintiff and Class Members would not have retained Defendant to provide healthcare services in the absence of an implied contract between them and Defendant obligating Defendant to not disclose Private Information without consent.

259. Defendant breached these implied contracts by disclosing Plaintiff's and Class Members' Private Information without consent to third parties like Facebook or Google.

260. As a direct and proximate result of Defendant's breaches of these implied contracts, Plaintiff and Class Members sustained damages as alleged herein, including but not limited to the loss of the benefit of their bargain and diminution in value of Private Information.

261. Plaintiff and Class Members are entitled to compensatory and consequential damages as a result of Defendant's breach of implied contract.

COUNT III
NEGLIGENCE
(On behalf of Plaintiff & the Nationwide Class)

262. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

263. Defendant owed Plaintiff and Class Members a duty to keep their Private Information completely confidential, and to safeguard sensitive personal and medical information.

264. Plaintiff and Class Members had reasonable expectations of privacy in their communications exchanged with Defendant, including communications exchanged on Defendant's Website.

265. Contrary to its duties as a medical provider and its express promises of confidentiality, Defendant installed its Tracking Technologies to disclose and transmit to third parties Plaintiff's and Class Members' communications with Defendant, including Private Information and the contents of such information.

266. These disclosures were made without Plaintiff's or Class Members' knowledge, consent, or authorization, and were unprivileged.

267. The third-party recipients included, but may not be limited to, Facebook and/or Google.

268. As a direct and proximate cause of Defendant's unauthorized disclosures of patient personally identifiable, non-public medical information, and communications, Plaintiff and Class members were damaged by Defendant's breach in that:

- a. Sensitive and confidential information that Plaintiff and Class members intended to remain private is no longer private;
- b. Plaintiff and Class members face ongoing harassment and embarrassment in the form of unwanted targeted advertisements;
- c. Defendant eroded the essential confidential nature of the provider-patient relationship;
- d. General damages for invasion of their rights in an amount to be determined by a jury;
- e. Nominal damages for each independent violation;
- f. Defendant took something of value from Plaintiff and Class Members and derived benefit therefrom without Plaintiff's and Class Members' knowledge or informed consent and without compensation for such data;
- g. Plaintiff and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality;
- h. Defendant's actions diminished the value of Plaintiff's and Class Members' Private Information; and

- i. Defendant's actions violated the property rights Plaintiff and Class Members have in their Private Information.

COUNT IV
Breach of Confidence
(On Behalf of Plaintiff & the Nationwide Class)

269. Plaintiff re-alleges and incorporates by reference the allegations above as if fully set forth herein.

270. Possessors of non-public medical information, such as CityMD, have a duty to keep such medical information completely confidential.

271. Plaintiff and Class Members had reasonable expectations of privacy in the responses and communications entrusted to CityMD through their Website, which included highly sensitive Private Information.

272. Contrary to their duties as telehealth institutions and their express promises of confidentiality, CityMD installed the Tracking Technologies to disclose and transmit to third parties Plaintiff's and Class Members' Private Information, including data related to Plaintiff and Class Members' health.

273. These disclosures were made without Plaintiff's or Class Members' knowledge, consent, or authorization.

274. The third-party recipients included, but may not be limited to, Facebook, Google, and other third parties.

275. As a direct and proximate cause of CityMD's unauthorized disclosures of Plaintiff's and Class Members' Private Information, Plaintiff and Class Members were damaged by CityMD's breach of confidentiality in that (a) sensitive and confidential information that Plaintiff and Class Members intended to remain private is no longer private; (b) Plaintiff and Class

Members face ongoing harassment and embarrassment in the form of unwanted targeted advertisements; (c) CityMD eroded the essential confidential nature of health services that Plaintiff and Class Members participated in; (d) general damages for invasion of their rights in an amount to be determined by a jury at trial; (e) nominal damages for each independent violation; (f) the unauthorized use of something of value (the highly sensitive Private Information) that belonged to Plaintiff and Class Members and the obtaining of a benefit therefrom without Plaintiff's and Class Members' knowledge or informed consent and without compensation to Plaintiff or Class Members for the unauthorized use of such data; (g) diminishment of the value of Plaintiff's and Class Members' Private Information; and (h) violation of the property rights Plaintiff and Class Members have in their Private Information.

COUNT V
Constructive Bailment
(On Behalf of Plaintiff & Nationwide Class)

276. Plaintiff re-alleges and incorporates by reference the allegations above as if fully set forth herein.

277. CityMD acquired and was obligated to safeguard the Private Information of Plaintiff and Class Members.

278. CityMD accepted possession and took control of Plaintiff's and Class Members' Private Information under such circumstances that the law imposes an obligation to safeguard the property of another.

279. CityMD accepted possession and took control of Plaintiff's and Class Members' Private Information under such circumstances that the law imposes an obligation to safeguard the property of another.

280. Specifically, a constructive bailment arises when CityMD, as is the case here, takes lawful possession of the property of another and has a duty to account for that property, without intending to appropriate it.

281. Constructive bailments do not require an express assumption of duties and may arise from the bare fact of the thing coming into the actual possession and control of a person fortuitously or by mistake as to the duty of ability of the recipient to affect the purpose contemplated by the absolute owner.

282. During the bailment, CityMD owed a duty to Plaintiff and Class Members to exercise reasonable care, diligence, and prudence in protecting their Private Information.

283. CityMD further breached its duty to safeguard Plaintiff's and Class Members' Private Information had been disclosed to third parties without Plaintiff's and Class Members' knowledge, consent, or explicit authorization.

284. As a direct and proximate cause of CityMD's breach of its obligations to safeguard their property, Plaintiff and Class Members have suffered compensable damages that were reasonably foreseeable to CityMD, including but not limited to, the damages set forth herein.

COUNT VI
Violation of the New York Deceptive Trade Practices Act
New York Gen. Bus. Law § 349, *et seq.*
(On Behalf of Plaintiff Andretta & the New York Subclass)

285. Plaintiff re-alleges and incorporates by reference the allegations above as if fully set forth herein.

286. By the facts and conduct alleged herein, CityMD committed unfair or deceptive acts and practices by:

- a. Promising to maintain the privacy and security of Plaintiff's and Class Members' PHI and/or PII as required by law;

- b. Installing the tracking technologies to operate as intended and transmit Plaintiff's and Class Members' Private Information without their authorization to Facebook, Google and other third parties;
- c. Failing to disclose or omitting material facts of Plaintiff and Class Members regarding disclosure of their Private Information to Facebook, Google and other third parties;
- d. Failing to take proper action to ensure the tracking technologies were configured to prevent unlawful disclosure of Plaintiff and Class Members' Private Information;
- e. Unlawfully disclosing Plaintiff's and Class Members' Private Information to Facebook, Google and other third parties.

287. These unfair acts and practices violated duties imposed by laws, including but not limited to, the Federal Trade Commission Act, HIPAA and NY GBL § 349.

288. CityMD's actions also constitute deceptive and unfair acts or practices because CityMD knew it failed to disclose to Plaintiff and the New York Class Members that their healthcare-related communications via the Website would be disclosed to Facebook, Google and other third parties.

289. CityMD's actions also constitute deceptive and unfair acts or practices because CityMD intended that Plaintiff and the New York Class Members relied on its deceptive and unfair practices and the concealment and omission of material facts in connection with CityMD's offering of goods and services.

290. Specifically, CityMD was aware that Plaintiff Andretta and the New York Class Members depended on and relied upon it to keep their communications confidential, and CityMD instead disclosed that information to Facebook.

291. In addition, CityMD's material failure to disclose that CityMD collects Plaintiff's and the New York Class Members' Private Information for marketing purposes with Facebook constitutes an unfair act of practice prohibited by the NY GBL § 349. CityMD's actions were immoral, unethical, and unscrupulous.

292. Plaintiff had reasonable expectations of privacy in her communications exchanged with CityMD, including communications exchanged via the Website.

293. Contrary to its duties as a medical provider and its express promises of confidentiality, CityMD deployed the Pixel to disclose and transmit Plaintiff's personally identifiable, non-public medical information and the contents of her communications exchanged with CityMD to third parties like Facebook.

294. CityMD's disclosures of Plaintiff Andretta and the New York Class Members' Private Information were made without their knowledge, consent, or authorization, and were privileged.

295. The harm arising from a breach of provider-patient confidentiality includes erosion of the essential confidential relationship between the healthcare provider and the patient.

296. CityMD willfully, knowingly, and intentionally and voluntarily engaged in the aforementioned acts when it incorporated the tracking technologies with knowledge of their purpose and functionality.

297. The harm described herein could not have been avoided by Plaintiff Andretta and the New York Class Members through the exercise of ordinary diligence.

298. As a result of CityMD's wrongful conduct, Plaintiff was injured in that she never would have provided her PII and/or PHI to CityMD or purchased CityMD's services, had she

known or been told that CityMD shared confidential and sensitive Private Information with Facebook.

299. As a direct and proximate result of CityMD's multiple violations of the GBL § 349, Plaintiff Andretta and the New York Class Members have suffered harm, including financial losses related to the payments or services made to CityMD that Plaintiff Andretta and the New York Class Members would not have made had they known of CityMD's disclosure of their PII and/or PHI to Facebook and other third parties, lost control over the value of their PII and/or PHI, including unwanted solicitations or marketing, entitling them to damages in an amount to be proven at trial.

300. CityMD's acts, practices, and omissions were done in the course of CityMD's business of furnishing healthcare-related services to consumers in the State of New York.

301. Plaintiff Andretta brings this action on behalf of herself and the New York Class Members are entitled to damages in an amount to be determined at trial, along with their costs and attorney's fees incurred in this action.

COUNT VII
UNJUST ENRICHMENT
(On behalf of Plaintiff & the Nationwide Class)

302. Plaintiff repeats and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

303. This claim is pleaded in the alternative to Plaintiff's common law claims.

304. Defendant benefits from the use of Plaintiff's and Class Members' Private Information and unjustly retained those benefits at their expense.

305. Plaintiff and Class Members conferred a benefit upon Defendant in the form of Private Information that Defendant collected from Plaintiff and Class Members, without

authorization and proper compensation to exceed the limited authorization and access to that information which was given to Defendant.

306. Plaintiff and Class Members conferred a monetary benefit upon Defendant in the form of valuable sensitive medical information that Defendant collected from Plaintiff and Class Members under the guise of keeping this information private. Defendant collected, used and disclosed this information for its own gain including for advertisement purposes, sale or trade for valuable services from third parties.

307. Plaintiff and Class Members would not have used Defendant's services or would have paid less for those services, if they had known that Defendant would collect, use, and disclose this information to third parties.

308. Defendant exceeded any authorization given and instead consciously disclosed and used this information for its own gain, providing Defendant with economic, intangible, and other benefits, including substantial monetary compensation.

309. Defendant unjustly retained those benefits at the expense of Plaintiff and Class Members because Defendant's conduct damaged Plaintiff and Class Members, all without providing any commensurate compensation to Plaintiff and Class Members.

310. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiff and Class Members.

311. As a result of Defendant's conduct, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in value between their purchases made with reasonable data privacy and security practices and procedures that Plaintiff and Class Members paid for, and those purchases without unreasonable data privacy and security practices and procedures that they received.

312. The benefits that Defendant derived from Plaintiff and Class Members was not offered by Plaintiff and Class Members gratuitously and rightly belongs to Plaintiff and Class Members. It would be against equity and good conscience for Defendant to be permitted to retain any of the profit or other benefits wrongly derived from the unfair and unconscionable methods, acts and trade practices alleged in this Complaint.

313. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds that Defendant received, and such other relief as the Court may deem just and proper.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Andretta, on behalf of herself and Class Members, requests judgment against CityMD and that the Court grant the following:

- A. For an Order certifying the Class and appointing Plaintiff and Counsel to represent such Class;
- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct alleged in this Complaint pertaining to the misuse and/or disclosure of the Private Information of Plaintiff and Class Members;
- C. For injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members;
- D. For an award of damages, including, but not limited to, actual, consequential, statutory, punitive, and nominal damages, as allowed by law in an amount to be determined;
- E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

- F. For prejudgment interest on all amounts awarded; and
- G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff Andretta hereby demands that this matter be tried before a jury.

DATE: June 14, 2024

Respectfully Submitted,

s/: David S. Almeida

David S. Almeida

New York Bar No. 3056520

Elena A. Belov

New York Bar No. 4080891

Matthew J. Langley

New York Bar No. 4831749

ALMEIDA LAW GROUP LLC

849 W. Webster Avenue

Chicago, Illinois 60614

Tel: (312) 576-3024

E: david@almeidalawgroup.com

E: elena@almeidalawgroup.com

E: matt@almeidalawgroup.com

Attorneys for Plaintiffs & the Classes